UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/051,495	01/18/2002	David Carroll Challener	RPS920010160US1	1606

7590 01/31/2006

DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, TX 78759

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/051,495	**Applicant(s)** CHALLENER ET AL.	
	Examiner Jeffery Williams	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 October 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 10/3/2005.

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Newly added claims, 16, 17, and 18, contain limitations for *"prior to evicting a parent cryptology key, determining how many child cryptology keys of the parent cryptology key will be disabled by the evicting of the parent cryptology key; and evicting from a plurality of parent cryptology keys a parent cryptology key that has been determined to affect fewer child cryptology keys that other parent cryptology keys in the plurality of parent cryptology keys."* The specification supports the determination of the number of "least keys" that will be affected by the eviction of an "evictable key", not the determination of the number of "child keys" affected by the eviction of a "parent key". The specification shows that the determination of the key to be evicted is based upon the affected "least keys" (keys used for message encryption/decryption vs. storage keys). Child keys may be either storage keys or "least keys". Not every child key of a parent is a "least key", the key used in the determination of an eviction. Furthermore, the specification discloses that an “evictable key” can be either a “storage key” or a “least key”. Thus, not every evictable key is a “parent key” – sometimes, an evictable key is a “least key”. The determination of key evictions based upon the number of “child keys” of a “parent key” is not supported by the specification.

Additionally, the implication that evicted parent keys “disable” child keys (*child cryptology keys of the parent cryptology key will be disabled by the evicting of the parent cryptology key*) lacks antecedent basis in the specification. The specification does not disclose child keys (inside or outside of the computer module) as being disabled, nor does the specification disclose a disabling of child keys by parent keys.

The examiner further points out that the disclosure is objected to because of the following informalities: Page 9, line 6, of the specification makes reference to “Figure 5” of the drawings. There is not a “Figure 5” found in the drawings. Appropriate correction is required.

Claim Objections

Claims 16 – 18 are objected to because of the following informalities: Line 5 of claim 16 contains the phrase “fewer child cryptology keys **that** other parent cryptology keys”. The examiner presumes the applicant to mean “fewer child cryptology keys **than** other parent cryptology keys”. Claims 17 and 18 are objected for similar reasons. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 16 – 18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See above rejection to the specification.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 – 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 ,6, and 11 each recites the limitation "said least expensive evictable cryptology key" in lines 12 or 13. There is insufficient antecedent basis for this limitation in the claim.

All other claims are rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 3, 5 – 8, 10 – 13, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trusted Computing Platform Alliance (TCPA), "Main Specification Version 1.0" in view of Challenger et al., "Algorithm for Cache Replacement", U.S. Patent 6,266,742 B1.

Regarding claim 6, TCPA discloses a trusted computing platform system, wherein exists a TPM ("computer module") designed to load, evict, and use cryptographic keys that are cached within the TPM (TCPA, pages 3, 5, 6; page 19, "TCPA_NOSPACE"; pages 38-40, 123-7, 136, 145-7). TCPA discloses that it is necessary for the TPM to utilize more keys than is allowable, due to constraints in storage space. Therefore, the trusted computing platform system provides a means for managing the loading of keys into the TPM. The keys are stored, or cached, inside the TPM in the form of a tree hierarchy of parent and children keys. Necessary keys utilized by the TPM, but stored outside of the device, are placed in encrypted key blobs (TCPA, page 123, pars. 1-3; page 124, lines 1-10). TCPA does not disclose the method in particular used by the trusted computing platform to efficiently manage which keys cached in the TPM or evicted from the TPM.

Challenger et al. discloses a method for managing objects stored in a cache. Challenger et al. discloses a means for determining a replacement expense for each of a plurality of cached objects in memory. The replacement expense is used to determine the desirability of caching or evicting an object from memory (Challenger et al., Abstract; fig. 4). The replacement expense is determined by a probability that each said evictable object will be needed by the computer module after said evictable object is evicted (Challenger et al., Abstract, lines 7), and an amount of cycle time required to re-store, if evicted, each said evictable object in the computer module (Challenger et al., Abstract, lines 7, 8; col. 1, lines 22-31). Challenger et al. further discloses a means for identifying a least expensive evictable object based on said replacement expense, and means for replacing said least expensive evictable object with a replacement object (Challenger et al., fig. 4, elems. 420, 460; TCPA, page 123, par. 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the method of Challenger et al. for efficiently managing a cache of stored objects with the system of TCPA for loading and evicting keys from a cache. This would have been obvious because one of ordinary skill in the art would have been motivated to manage the loading and evicting of objects ("keys") from the TPM in a manner characterized by the efficient utilization of system processes.

Regarding the amendment of claim 6, specifically the added limitation for the determination of the replacement expense including the *calculating a number of generations to a nearest ancestor that is required to unwrap said least expensive* *evictable cryptology key,* the combination of TCPA and Challenger disclose the determination of the replacement expense including the determination of the *time (t) necessary to fetch or calculate* an object (key) (Challenger et al., col. 1, lines 28-32; col. 4, lines 2-6, 56-61). The combination of TCPA and Challenger discloses that this determination of the time (t) necessary to fetch an object applies within an environment of hierarchical data structures consisting of parents and children (Challenger et al., col. 3, lines 52-67; TCPA, page 124, lines 1-7, bullets 1, 3-5; page 125, bullet 4; page 126, bullet 9; page 127, bullet 1; page 145). As taught by the combination of TCPA and Challenger, keys exist in a hierarchical tree structure of parents and children. To load a child key into a computer module, the computer module must first possess the parent key of the child key (TCPA, page 124). When a target key is desired to be loaded, the computer module must possess at least any one of a plurality of ancestor keys of the child key in the key hierarchy (TCPA, page 127). Thus, it is clear; to load a child key, one needs the parent key. A parent key is used to load a child key. If that parent key is not possessed, one requires at least any one of a plurality of ancestor keys in the hierarchy. With an ancestor key (a parent key) one may load the child of that ancestor. Accordingly, the process continues until the desired child key is capable of being loaded using its parent key, the parent key itself being a child of an ancestor.

It is clearly logical, to anyone of ordinary skill in the art that this is an ordered process. While the combination of TCPA and Challenger does not explicitly use the phrase "*calculating a number of generations to a nearest ancestor*", the combination discloses determining the time necessary to calculate or fetch a child key using any one of a plurality of close or distant ancestors. Logically, the time to load a child key will be longer if only a distant ancestor is possessed as opposed to if the immediate parent of the child key is possessed, the time to load being dependent upon the number of ancestral parents (generations) between the child and the possessed parent. This is logical, as the process that requires more loads is longer than the process that requires less loads. Thus, It would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to recognize that the time necessary to load a child key depends upon the number of upon the number of ancestral parents (generations) between the child and the nearest ancestor.

Regarding claim 7, the combination of TCPA and Challenger et al. discloses:

means for locating a blob comprising said least expensive evictable cryptology key and a security software shell; means for removing said security software shell from said blob; and means for storing said least expensive evictable cryptology key in said computer module (Challenger et al., page 124).

Regarding claim 8, the combination of TCPA and Challenger et al. discloses:

wherein an expense to re-load an evictable cryptology key is determined by both an expense to reload a child evictable cryptology key as well as an expense to reload any ancestor cryptology keys of the child evictable cryptology key (See rejection of claim 6, Challenger et al., col. 1, lines 28-32; col. 4, lines 2-6, 56-61; TCPA, pages 124-127).

Regarding claim 10, the combination of TCPA and Challenger et al. discloses: *wherein the computer module is a Trusted Platform Module (TPM)* (TCPA, page. 123).

Regarding claim 17, the combination of TCPA and Challenger et al. discloses a system for managing the removal or detention of keys within a computer module (See rejection of claim 6, Challenger et al., col. 4, lines 32-36; col. 1, lines 28-32; col. 4, lines 2-6, 56-61; TCPA, pages 124-127). The combination discloses that it is important to consider, when making decisions for the removal or detention of keys, the probability of an object being needed by the module in the future. The combination, however, does not disclose that the decision to remove a key is based upon the number of system keys that will be affected by its removal from the computer module. However, it would have been obvious to one of ordinary skill in the art to consider this factor when removing keys from the device. This would have been obvious, because one of ordinary skill in the art would have recognized that data (keys) arranged in a hierarchical tree structure causes for the interdependency of structural elements, data (keys). Thus, one of ordinary skill in the art would logically want to make the change that causes the least detrimental affect to the structural functionality as a whole.

Regarding claims 1 – 3, 5, 11 – 13, 15, 16, and 18, they are the method and computer program product claims implemented by and corresponding to the system claims 6 – 8, 10, and 17, and they are rejected for the same reasons.

Claims 4, 9, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Trusted Computing Platform Alliance (TCPA), "Main Specification Version 1.0" and Challenger et al., "Algorithm for Cache Replacement", U.S. Patent 6,266,742 B1 as applied to claims 1 – 3, 5 – 8, 10 – 13, and 15 above, and further in view of Deshpande et al., "Method of Reconstructing a Managed Information Tree", U.S. Patent 5,893,103.

Regarding claim 9, the combination of TCPA and Challenger et al. disclose a system for the loading (caching) of keys organized into hierarchal data structures into a TPM (see rejections of claims 6, 7, and 8). The combination of TCPA and Challenger et al. does not disclose in particular the method for the loading of a hierarchal structure of keys.

Deshpande et al., discloses a method for replicating into memory a hierarchal structure of objects from a remote location. Deshpande et al. discloses a means for methodically loading and storing the ancestor objects of a child object until the hierarchal structure is established so that the child object itself may be loaded and stored (Deshpande et al., col. 4, lines 18-44).

It would have been obvious to one of ordinary skill in the art to employ the method of Deshpande et al. for replicating in memory a hierarchal structure of data in the system of the combination of TCPA and Challenger et al. for the loading and caching of parent and children keys. This would have been obvious because one of ordinary skill in the art would have been motivated to employ a method enabling the loading of ancestor keys into memory so that a necessary child key may be loaded.

Regarding claims 4 and 14, they are the method and computer program product claims implemented by and corresponding to the system claims 9, and they are rejected for the same reason.

Response to Arguments

Applicant's arguments filed 10/3/05 have been fully considered but they are not persuasive.

Applicant's argue primarily that:

I. *With regards to exemplary Claim 1, the cited art does not teach or suggest determining a cycle time required to re-store an evictable cryptology key by cycle time is determined by calculating a number of generations to a nearest ancestor that is* *required to unwrap said least expensive evictable cryptology key, said nearest ancestor being from a plurality of non-evicted remaining cryptology keys in the computer module," as supported, inter alia, on pages 8-9 of the present specification* (Remarks, page 11, par. 1).

In response, the examiner encourages the applicant to consider the above rejection of claim 1.

II. *Challenger teaches a method for determining which value to replace in cache. Part of the equation taught on column 4 of Challenger uses "a" which is the expected time between successive requests" for an object (Challenger, col. 4, lines 60-61). However, there is no teaching or suggestion that this time is based on "calculating a number of generations to a nearest ancestor cryptology key that is required to unwrap said least expensive evictable cryptology key."* (Remarks, page 11, par. 3).

Similarly, in the passages from Challenger cited in the present Office Action (including col. 1, lines 28-32 and col. 3, lines 52-67), Challenger teaches that caching of objects may depend on "the frequency with which an object is accessed, object size, the time to calculate an object, or the time to fetch the object from a remote location, and the lifetime (i.e., time between updates) of an object." (Challenger, col. 1, lines 28-32.) The Examiner cites this passage as disclosing "as obvious that fact that calculating the time necessary to fetch an object would include the time it takes to fetch the ancestors *of which the object depends upon in the hierarchal data structure." (Page 5, lines 18-20 of the present Office Action.)* (Remarks, page 11, par. 4).

Applicants respectfully traverse Examiner's contention. The cited art does not teach or imply "calculating a number of generations to a nearest ancestor cryptology key that is required to unwrap said least expensive evictable cryptology key" because the cited art never mentions or implies considering ancestors at all, much less ancestor objects used to unwrap children objects. It is axiomatic that the prior art must teach or suggest all of the limitations found in the presently presented claim. (Remarks, page 12, par. 1).

In response, the examiner encourages the applicant to reconsider the prior art rejection, including the reference of Challenger. Contrary to the applicant's implication that the reference of Challenger is applicable only in teaching the use "a" (time between requests), consideration of Challenger also teaches the use "t", representing the estimated time to calculate or fetch an object.

Additionally, the rejection of claims 1, 6, and 11 are made in view of the combination of TCPA and Challenger. The Applicants, however, neglect to address the rejection with respect to the combination of TCPA and Challenger, and focus solely on the teachings of Challenger. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re*

Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

III. The prior art does not teach or suggest the limitations of claims 3, 8, and 13 (Remarks, page 12, par. 3).

In response, the examiner invites the applicant to consider the above rejection of claims 3, 8, and 13.

IV. The prior art does not teach or suggest the limitations of claims 16 – 18 (Remarks, page 12, par. 4).

In response, the examiner invites the applicant to consider the above rejection of claims 16 – 18.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER